

# SOPHOS



## sophos **anti-virus**

### User manual

Sophos Anti-Virus for OS/2

For networked and single computers

Document date: February 2007





# Contents

About this manual	4
<b>Using Sophos Anti-Virus</b>	
1 Using Sophos Anti-Virus via the GUI	6
2 Using Sophos Anti-Virus via the CLI	13
3 Using InterCheck	16
4 Disinfection	19
<b>Configuration</b>	
5 Immediate and scheduled scanning options (GUI)	28
6 Global configuration options (GUI)	39
7 Configuration via the CLI	44
8 Configuring InterCheck	67
<b>Troubleshooting</b>	
9 Troubleshooting	74
<b>Glossary and index</b>	
Glossary	78
Index	80
Technical support	82

## About this manual

This user manual explains how to use Sophos Anti-Virus for OS/2 and how to configure

- virus scanning
- virus alerts
- reporting
- disinfection
- logging.

The manual also provides help in resolving common problems.

For information on the installation, initial setup, updating or uninstallation of Sophos Anti-Virus on an OS/2 network, see the *Sophos Anti-Virus OS/2 computers on a network installation guide*.

For information on the installation, initial setup, updating or uninstallation of Sophos Anti-Virus on a single OS/2 computer, see the *Sophos Anti-Virus OS/2 single user installation guide*.

Sophos documentation is published on the **Sophos Anti-Virus Supplementary CD** and at [www.sophos.com/support/docs/](http://www.sophos.com/support/docs/)

# ***Using Sophos Anti-Virus***

**Using Sophos Anti-Virus via the GUI**

**Using Sophos Anti-Virus via the CLI**

**Using InterCheck**

**Disinfection**

# 1 Using Sophos Anti-Virus via the GUI

This section contains the following information about using Sophos Anti-Virus for OS/2 via the GUI.

- Overview of the **Sophos Anti-Virus** window (section 1.1).
- Running an immediate scan (section 1.2).
- Scheduling scans (section 1.3).

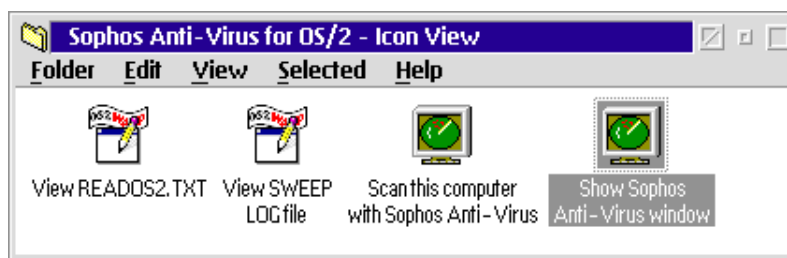
## 1.1 Overview of the Sophos Anti-Virus window

### 1.1.1 Opening the Sophos Anti-Virus window

1. On the desktop, double-click the **Sophos Anti-Virus for OS/2** icon.

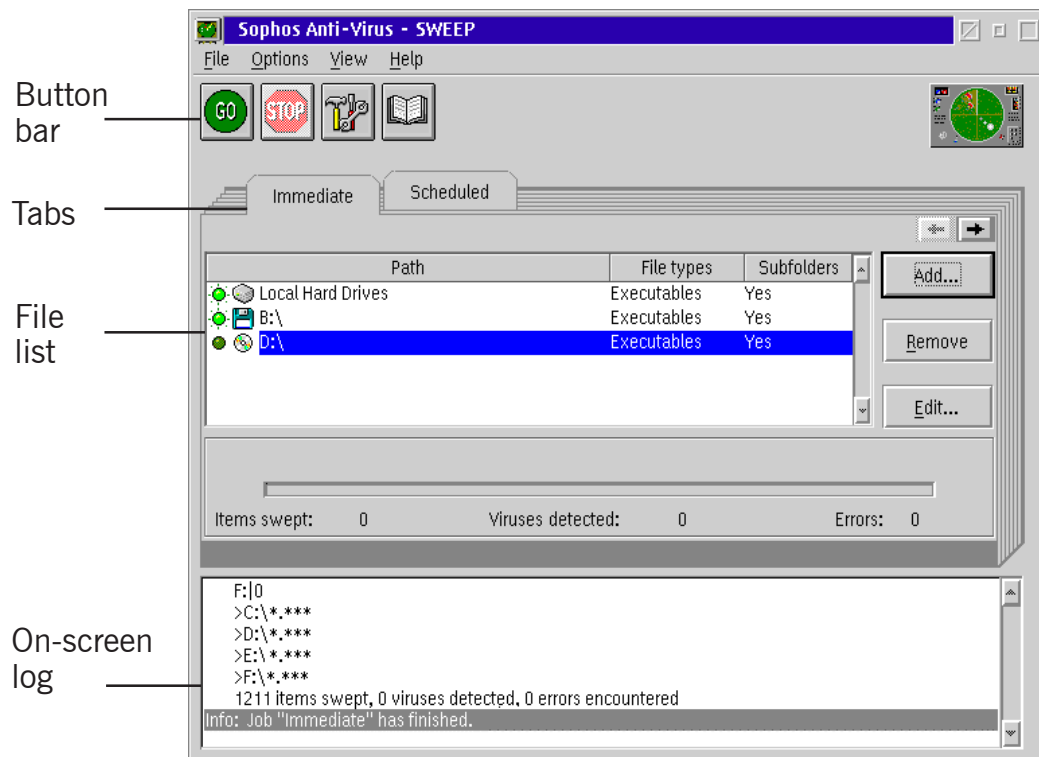


2. In the **Sophos Anti-Virus for OS/2** folder, double-click the **Show Sophos Anti-Virus window** icon.



- 💡 To scan the computer immediately, double-click the **Scan this computer with Sophos Anti-Virus** icon.

## 1.1.2 Features of the Sophos Anti-Virus window



### Button bar



Starts a scan.



Ends a scan.



Opens a dialog box in which you can configure Sophos Anti-Virus.



Connects you to the Sophos virus analyses on the Sophos website.

### Tabs

There is a tabbed page for each type of scan:

**Immediate** for scanning on demand.

**Scheduled** for scanning automatically at set times.

You cannot control or configure InterCheck on-access scanning via the **Sophos Anti-Virus** window. See [section 8](#) for information about configuring InterCheck.

### **File list**

On the **Immediate** tabbed page, the file list shows items that can be scanned. An illuminated light to the left of an entry indicates that it will be included in an immediate scan. Click this light to select or deselect items.

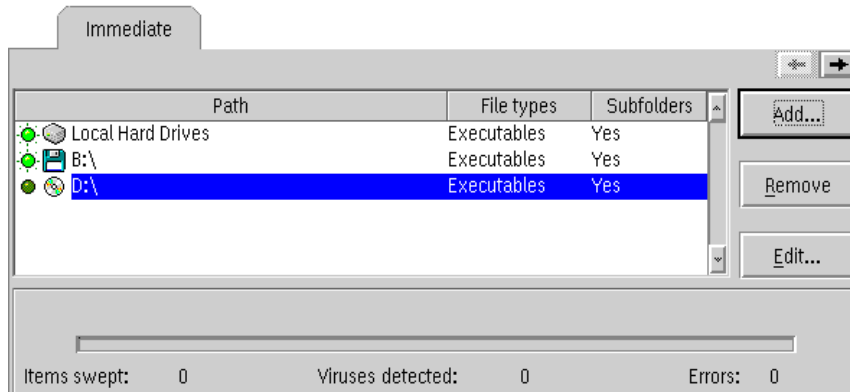
On the **Scheduled** tabbed page, the file list is replaced with the scheduled job list. This is the list of scheduled scans configured to take place on the computer.

### **On-screen log**

The on-screen log contains information about the current session, along with all log messages since the window was opened. Double-clicking on a virus name here connects you to an analysis of the virus on the Sophos website.

## 1.2 Running an immediate scan

To run an immediate scan, first ensure the **Immediate** tabbed page is selected.



The path list shows the drives, paths and files that can be scanned in an immediate scan. An illuminated light to the left of an item indicates that it will be scanned. Click this light to select or deselect items.

### 1.2.1 Starting an immediate scan

To scan all the selected drives, click **GO**.



To scan *an individual item* in the area list, whether the light beside it is illuminated or not, double-click that item.

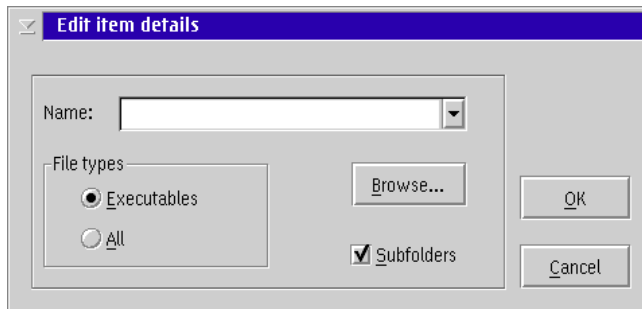
### Interrupting scanning

To stop scanning at any time, click **STOP**.



### 1.2.2 Adding and editing items for immediate scanning

To add new items for immediate scanning, or edit existing items, ensure the **Immediate** tabbed page is selected and click the **Add** or **Edit** button. The **Edit item details** dialog box is displayed.



#### Path name

Specifies the drive, folder or filename to be scanned. Both drive-mapped and UNC path names can be entered. Wildcards can also be included. Click **Browse** to select from a list of available items. Use the drop-down menu to select **Local hard drives**, rather than specific paths.

#### File types

By default, only files defined as executables are scanned, unless you select **All**. To find out how to change the list of files defined as executables, see [section 6.2](#).

#### Subfolders

Select this option to scan subfolders.

### 1.2.3 Removing items for immediate scanning

Highlight (by clicking) the name of the path to be removed and click the **Remove** button.

## 1.3 Scheduling scans

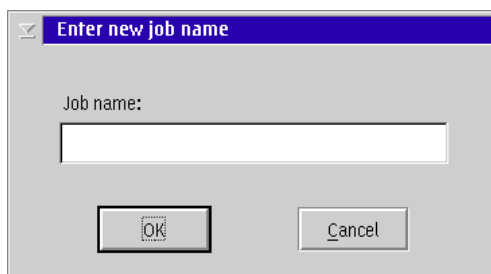
To view or edit scheduled jobs, first ensure the **Scheduled** tabbed page is selected.

### 1.3.1 Default scheduled mode job list

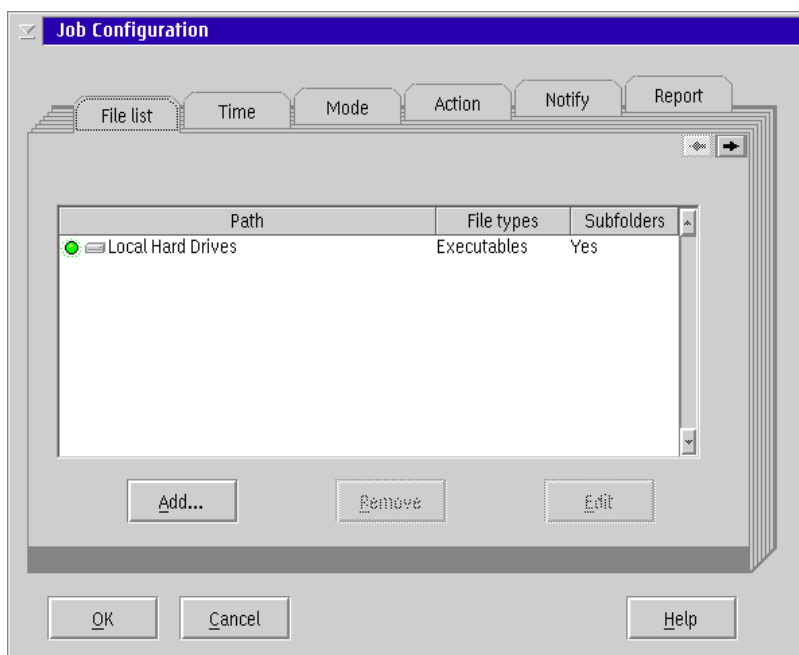
By default, there is a job named 'Default', which scans all local hard drives. See [sections 1.3.3 and 1.3.4](#) for details of how to modify or remove this job.

### 1.3.2 Adding a new scheduled job

1. Click the **Add** button on the **Scheduled** tabbed page.
2. Enter the name of the job in the **Enter new job name** dialog box.



3. In the **Job Configuration** dialog box, use the tabs to set up the job.



The options in the **Job Configuration** dialog box are explained in [section 5](#).

### **1.3.3 Editing a scheduled job**

Highlight (by clicking) the name of the scan and click the **Edit** button, or double-click the name of the scan. The **Job Configuration** dialog box is displayed, in which you can edit the scan.

### **1.3.4 Removing a scheduled job**

Highlight (by clicking) the name of the job to be removed and click the **Remove** button.

## 2 Using Sophos Anti-Virus via the CLI

This section describes how to run immediate scans from the command line on workstations or on a file server.

- ❗ This section describes how to run immediate scans with the default settings. In most cases, these settings are sufficient. To find out how to change the default settings, see [section 7](#).

### 2.1 What are the defaults?

By default, Sophos Anti-Virus will look for viruses in:

- nearly 50 types of file identified by their filename extension
- logical sector 0 of all local hard disk drives
- physical sector 1 of hard disk devices 80 to 83 Hex.

See [section 7](#) to find out how to change these defaults.

#### Scanning level

By default, Sophos Anti-Virus performs a quick scan, which checks only those parts of files likely to contain viruses. This is usually sufficient. See [section 7.6](#) for details.

### 2.2 Scanning hard disks

Enter the command

```
OSWEEP
```

This starts a scan of all local hard drives. To interrupt the scan, press 'Esc' at any time.

To scan specific local or network hard drives, use their letters. For example

```
OSWEEP D: E:
```

If a virus is found, a red warning message is displayed at the end of the scan. To clear the warning, press any key. The names of viruses discovered are then displayed.

## 2.3 Scanning floppy disks

Enter the command

```
OSWEEP -MU A:
```

You are then prompted to insert the disks you want to scan.

## 2.4 Scanning file servers

You can scan file server logical drives over a network. On most networks it is necessary to be logged in as a supervisor or have read rights equivalent to those of a supervisor (the latter is more secure if the workstation itself is infected).

Most networks do not allow file server boot sectors to be examined. Sophos Anti-Virus determines automatically to which network drives such restrictions apply. You can force Sophos Anti-Virus to treat all drives as network drives during a scan by using the `-FS` command line qualifier.

On most networks, some files are not readable and Sophos Anti-Virus will report an error when it tries to open them. It automatically avoids the files

```
\EA#DATA.#SF  
\WP#ROOT.#SF  
\OS2\SYSTEM\SWAPPER.DAT
```

on all drives (where the `#` symbol represents the space character).

Any files can be exempted from a scan by quoting them, preceded by the **exclusion operator**, in the SWEEP.ARE file. For more information see [section 7.4](#).

A quick way to find unreadable files on the file server is to run a scan and note the names of any file(s) that could not be opened.

- 💡 Maximum effectiveness is obtained by running Sophos Anti-Virus on the file server itself in stand-alone mode. For instructions on disinfecting a system in stand-alone mode, see [section 4.2](#).

## 2.5 Running Sophos Anti-Virus on a file server

Sophos Anti-Virus for OS/2 can be installed on a LAN Server or LAN Manager file server as an integral part of an anti-virus strategy. Although Sophos Anti-Virus does not contain any network-specific features, the LAN server environment encourages the use of different techniques for controlling the operation of the virus scanner.

### Scheduling

You can schedule regular scans using the AT command, provided by the Network Operating System. For example, the following instruction will run a scan at midnight each day and place the output in the file OSWEEP.LOG:

```
AT 00:00 /E:M,T,W,Th,F,S,Su "C:\SAV\OS2SWEEP\ENG\OSWEEP -P=C:\SAV\OSWEEP.LOG"
```

The red alert message is displayed if a virus is detected. The log file should then be examined to determine which files are infected. Full pathnames must be specified. The instruction can be added to the startup command file so that it will be executed automatically every time the server is started.

### Background Operation

Sophos Anti-Virus can be configured to run continually as a background process. A command file is required to restart the scan. The following is a simple example file that scans continuously until a virus is detected.

```
@ECHO OFF
:START
C:\SAV\OS2SWEEP\ENG\OSWEEP -PR=L -P=C:\SAV\OSWEEP.LOG
IF ERRORLEVEL 3 GOTO VIRUS_FOUND
GOTO START
:VIRUS_FOUND
```

The qualifier

```
-PR=L
```

changes the priority of the scan to low, so that the impact on server performance is reduced. It is not advisable to run the command file as a detached process since it cannot easily be monitored or terminated. The command should be run in the background instead. To ensure the command file is executed every time the server is started, add the following line to the startup command file

```
START /MIN RUNSWEEP.CMD
```

where RUNSWEEP.CMD is the command file.

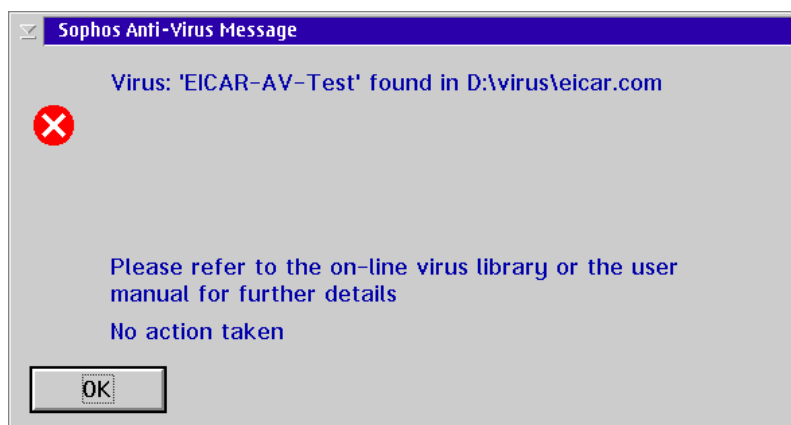
The command file can easily be customised to take additional actions when a virus is encountered.

## 3 Using InterCheck

InterCheck checks files for viruses as they are accessed by the computer, and denies access to a file if it contains a virus. InterCheck also scans removable disks for boot sector viruses, and denies access to a whole disk if it contains an infected boot sector. To find out how to configure InterCheck, see [section 8](#).

- ❗ **Do not run more than one on-access scanner at any one time. This could cause serious problems with your system, or even prevent OS/2 from booting.**

If InterCheck finds a virus, it displays a message like this:



Click **OK**. Deal with the virus as explained in [section 4](#).

Notification to network administrators of viruses is done using the network's native messaging utility. When infected files are accessed frequently, in extreme cases the capacity of the messaging system may be exceeded. Although this means some infected files may not be reported to the network administrator, they will be made aware of which computers store infected files. They can then check the InterCheck log on those computers, which contains a definitive record of all viruses found and other important events.

Running InterCheck can slow down a computer, especially when it is starting up. To avoid this, configure the OS/2 file systems to use large caches, using the command `DISKCACHE=` and/or the `/CACHE=` qualifier of the `IFS=` command in `CONFIG.SYS`. Sophos recommends a value of 2048 in each case, or 1024 if computer memory is limited. See the IBM OS/2 Command Reference Guide for more information.

InterCheck does not scan the contents of archive files before the archive files are unpacked. (However, it does scan the extraction 'stub' of self-extracting

archives prior to extraction.) This is because such a process could be too slow for an on-access scanner. After archive files have been unpacked with the archive utility, InterCheck prevents access to any of the unpacked files that are infected, so that security is maintained.

Sophos does not recommend using InterCheck on a file server as it is likely to reduce performance. Files held on servers will be scanned by clients running InterCheck when they access the files.

InterCheck is designed to prevent multiple virus alerts due to repeated attempts by a user to access the same infected file. For more information, see the **InfectedCacheLifetime=** command in [section 8](#).

InterCheck only scans files when they are opened: it does not scan them when they are closed. In practice, this means that files are scanned before they are read, not when they are created.

InterCheck does not automatically disinfect infected items.

Because the standard releases of OS/2 are not high security products, InterCheck does not give complete security against the activities of malicious users (e.g. a knowledgeable user can disable InterCheck on their computer). InterCheck is believed to be compatible with third-party security products that use the OS/2 Installable Security Subsystem. Where such a product is installed, it is possible that it could be used to protect InterCheck against malicious users. However, Sophos does not endorse any such product.

It is not necessary to disable the 'opportunistic lock' feature of IBM LAN Server networking to enable InterCheck to work. This is of particular significance for computers running IBM Peer Server.

### 3.1 Monitoring InterCheck

To confirm that InterCheck is active, in the **InterCheck Monitor** window, check the **Status** field.



By default, InterCheck Monitor is launched on OS/2 at bootup.

If it is not running, on the desktop, in the **Sophos Anti-Virus for OS/2** folder, double-click **InterCheck Monitor**.

InterCheck Monitor displays

- the total number of items filtered (i.e. checked against the list of authorised items by InterCheck)
- the status of InterCheck (active or inactive)
- the last item filtered.

To display the InterCheck Monitor menu, click the left-hand side of its title bar. You can open the **Sophos Anti-Virus** window from this menu.

- 🔗 Closing InterCheck Monitor does not stop InterCheck.

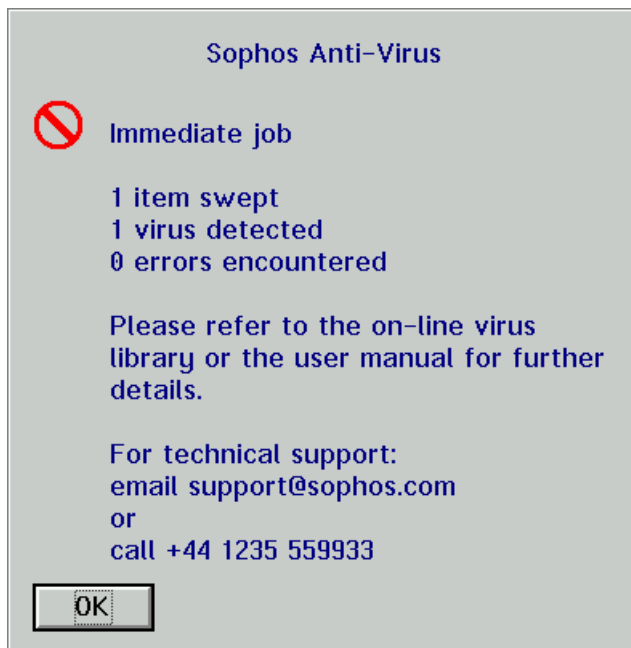
## 4 Disinfection

This section provides some general information about disinfection. ***It does not explain how to disinfect a computer of specific viruses***, as disinfection methods are varied and can be virus-specific.

- ❗ **It is recommended that you get information about the virus (see below), then either use the Sophos website for help with disinfection or contact Sophos [technical support](#).**

### 4.1 Getting information about the virus

If the Sophos Anti-Virus GUI finds a virus, it displays a message box like this:



You also see details in the on-screen log at the bottom of the **Sophos Anti-Virus** window.

If command line Sophos Anti-Virus finds a virus, it displays a message like this:

```
Sophos Anti-Virus
Version 3.90.0
Virus data version 3.90, February 2005
Includes detection for 99603 viruses, trojans and worms
Copyright (c) 1989-2005 Sophos Plc, www.sophos.com

System time 20:16:25, System date 16 February 2005

Quick Sweeping
Press Esc to quit

>>> Virus 'EICAR-AV-Test' found in file F:\EICAR.COM

9 files swept in 0 minutes and 1 second.
1 virus was discovered.
1 file out of 9 was infected.
```

For advice consult [www.sophos.com](http://www.sophos.com), email [support@sophos.com](mailto:support@sophos.com) or telephone +44 1235 559933

First isolate the infected computers from the network and internet.

Write down the name of the virus. Then, from an uninfected computer, look up its virus analysis on the Sophos website. The virus analysis search page is located at

[www.sophos.com/virusinfo/analyses](http://www.sophos.com/virusinfo/analyses)

- ❗ You can go straight to this page by double-clicking the **Sophos Virus Information Website** icon in the **Sophos Anti-Virus for OS/2** folder.

The analysis tells you what types of files the virus infects, and provides information about disinfection. It may also include a link to detailed disinfection instructions. Use these instructions to help you disinfect the computer. If there are no instructions, contact Sophos [technical support](#).

## 4.2 Disinfection

Sophos Anti-Virus's automatic disinfection facilities, or OS/2 commands, can deal with most virus attacks.

- **Infected boot sectors** can be disinfected (in some cases) or disabled.
- **Infected documents** can be disinfected.
- **Some infected programs** can be disinfected.
- **Infected files** can be deleted.

- ❗ You cannot disable boot sectors from the Sophos Anti-Virus GUI.

If you are using the **Sophos Anti-Virus** window, specify automatic disinfection in the **Job Configuration** dialog box (described in [section 5.4](#)). Then run an immediate scan of the infected area (described in [section 1.2](#)).

If using Sophos Anti-Virus from the command line, or if automatic disinfection is unsuccessful, see the rest of this section for more information about disinfection.

#### 4.2.1 Dealing with boot sector viruses on the hard disk

There are two ways to deal with boot sector viruses on the hard disk; by disinfection or by replacing the boot sector.

##### Disinfection

This is the preferred approach. Before disinfection, backup any important data on the hard disk. This procedure assumes that A: is the floppy disk and E: is the CD.

1. If OS/2 is already running, shut it down.
2. Boot OS/2 from the OS/2 Utility disk set. The disks should include a CD driver and the following files: NLS.DLL, QUECALLS.DLL, and VIOCALLS.DLL. Follow the on-screen instructions. When booting is finished, the A: prompt appears.
3. Insert the **Sophos Anti-Virus Supplementary CD**.
4. At a command prompt, enter

```
SET BEGINLIBPATH=A:\;E:\OS_2
```

This tells OS/2 where to find the files mentioned in step 2.


5. Enter

```
E:\OS_2\OSWEEP -DI
```

The computer is scanned for boot sector and file viruses. Sophos Anti-Virus disinfects infected boot sectors and some programs (see [section 4.2.3](#)). If this procedure fails to disinfect a virus on your computer, contact [Sophos technical support](#).

## Replacing the boot sector

In most cases, the boot sector can be overwritten with a clean one.

1. Check that the contents of the infected drive are visible (e.g. with DIR).
1.  If the contents of the hard disk are not visible, contact Sophos [technical support](#) for advice. Some boot sector viruses require additional action for full recovery.
2. **To overwrite the master boot sector**, ensure the last OS/2 Utility Disk is in the drive and enter:

```
FDISK /NEWMBR
```

or, in the case of Warp Server for e-business or Warp 4 Convenience Packages

```
LVM /NEWMBR
```

**To overwrite the OS/2 boot sector**, locate the OS/2 Utility disk containing the file SYSINSTX.COM.

- For Warp 3 and Warp Server v4, this will be the third of the three Utility disks.
- For Warp 4 (Merlin), Warp Server for e-business and Warp 4 Convenience Packages, this will be the first of the four Utility disks.

Insert this disk in drive A: and enter a command such as:

```
SYSINSTX C:
```

### 4.2.2 Dealing with boot sector viruses on floppy disk

Floppy disks with infected boot sectors can be either disinfected or reformatted.

#### Disinfection

This procedure assumes that A: is the floppy disk and E: is the CD.

1. If OS/2 is already running, shut it down.
2. Boot OS/2 from the OS/2 Utility disk set. The disks should include a CD driver and the following files: NLS.DLL, QUECALLS.DLL, and VIOCALLS.DLL. Follow the on-screen instructions. When booting is finished, the A: prompt appears.
3. Insert the **Sophos Anti-Virus Supplementary CD**.

4. At a command prompt, enter

```
SET BEGINLIBPATH=A:\;E:\OS_2
```

This tells OS/2 where to find the files mentioned in step 2.

5. Enter

```
E:\OS_2\OSWEEP A: -DI -MU
```


6. When the computer prompts you, insert the floppy disks to be disinfected. Infected boot sectors and programs are disinfected.
7. When disinfection is complete, scan the whole computer for remaining infections.

If this procedure fails to disinfect a virus on your floppy disk, contact Sophos [technical support](#).

### Reformatting

1. If OS/2 is already running, shut it down.
2. Boot OS/2 from the OS/2 Utility disk set. Follow the on-screen instructions. When booting is finished, the A: prompt appears. Remove the OS/2 Utility disk.
3. Copy the valuable data from the infected disk to a clean destination (it is safe to copy files if the computer has been clean booted).
4. Reformat the infected disk.

### 4.2.3 Dealing with infected programs

 Sophos Anti-Virus can disinfect some infected programs. However, disinfected programs may be unstable, and put valuable data at risk. We recommend that disinfection of programs is used only as a temporary measure, and that you subsequently replace disinfected programs from original installation disks, a clean computer or sound backups.

1. To disinfect an infected program, enter

```
OSWEEP [PROG.EXE] -DI
```

where [PROG.EXE] is the program name.

2. Scan the whole computer for remaining infections.

3. If the program cannot be disinfected, delete the program using

```
OSWEEP [PROG.EXE] -REMOVEF
```

and replace it from original installation disks, a clean computer or sound backups. The virus may have corrupted it.

-REMOVEF affects infected files only, and can be used on network drives from the workstation. It does not require OS/2 to be shut down, unless a file to be removed is locked (e.g. an OS/2 system file). In this case, contact Sophos [technical support](#).

If the -RS qualifier is specified as well, infected files will be positively overwritten rather than simply deleted. This makes them irrecoverable.

In either case, you are asked to confirm that each file should be removed, unless the -NOC (No confirmation before virus removal) qualifier is used.

#### 4.2.4 Dealing with infected documents

When dealing with infected documents, it is not necessary to reboot from a clean system disk. However, it is important to ensure that the application that created the document is not open when disinfection is attempted.

To disinfect a document file, use a command such as

```
OSWEEP FILE.DOC -DI
```

In some cases, it is possible to manually edit the macros from the infected document using the relevant application. However, some macro viruses now operate a form of stealth to prevent users from doing this. For example, Winword/ShareFun disables the **Macro** option on the **Tools** menu, and **Templates** option on the **File** menu. Consult Sophos [technical support](#) before attempting to perform manual disinfection of macro viruses.

#### 4.2.5 Dealing with an infected Boot Manager

Almost all known viruses execute in DOS mode. OS/2 systems with Boot Manager configured are vulnerable to attack while DOS is running. For example, the common virus Form can damage the Boot Manager.

If the OS/2 Boot Manager is infected, do as follows. This procedure assumes that A: is the floppy disk and E: is the CD.

1. If OS/2 is already running, shut it down.
2. Boot OS/2 from the OS/2 Utility disk set. The disks should include a CD driver and the following files: NLS.DLL, QUECALLS.DLL, and VIOCALLS.DLL. Follow the on-screen instructions. When booting is finished, the A: prompt appears.

3. Insert the **Sophos Anti-Virus Supplementary CD**.

4. At a command prompt, enter

```
SET BEGINLIBPATH=A:\;E:\OS_2
```

This tells OS/2 where to find the files mentioned in step 2.

5. Enter

```
E:\OS_2\OSWEEP -DI
```

The computer is scanned for boot sector and file viruses. Sophos Anti-Virus disinfects infected boot sectors and some programs (see [section 4.2.3](#)). If this procedure fails to disinfect Boot Manager, continue to step 6.

6. Ensure the last OS/2 Utility Disk is in the drive.
7. Use the OS/2 FDISK (or LVM) utility to delete and reinstall the Boot Manager. Detailed instructions are in IBM's OS/2 documentation. If this procedure fails to disinfect Boot Manager, contact Sophos [technical support](#).

### 4.3 Recovering from virus side effects

How you recover from a virus infection depends on how the virus affected the infected computer. Some viruses leave you with no side effects to deal with. Others have such extreme side effects that you have to restore a hard disk or replace the BIOS in order to recover.

Some viruses gradually make minor changes to data. This type of corruption can be very hard to detect. Read the virus analysis on the Sophos website [www.sophos.com](http://www.sophos.com), and check files carefully after disinfection.

Sound backups are crucial. If you did not have them before you were infected, ensure you create or obtain them in case of future infections.

Sometimes you can recover data from disks damaged by viruses. Sophos can supply utilities for repairing the damage caused by some viruses. Contact Sophos [technical support](#) for help.



# ***Configuration***

**Immediate and scheduled scanning options (GUI)**

**Global configuration options (GUI)**

**Configuration via the CLI**

**Configuring InterCheck**

## 5 Immediate and scheduled scanning options (GUI)

This section describes how to configure two modes of scanning:

- Immediate scanning.
- Scheduled scanning (for which you specify a different configuration for each scheduled job).

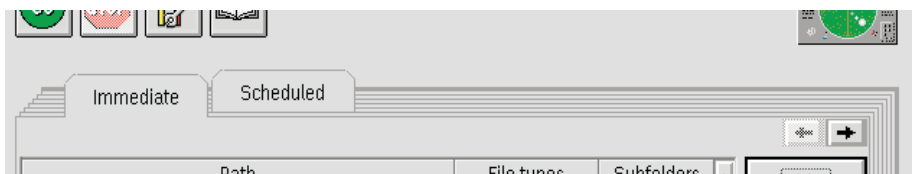
The different scanning modes are described in [section 1](#).

This section also describes how to set up scheduled scanning on multiple computers on the network.

For information on further, global options (e.g. to exclude files from all forms of scanning), see [section 6](#).

There are **Job Configuration** dialog boxes for immediate scanning and each scheduled job. They enable you to specify which items Sophos Anti-Virus should scan and what action it should take on discovering a virus.

To open the required configuration dialog box, in the **Sophos Anti-Virus** window, click the tab for the scanning mode you would like to configure.



If you clicked the **Scheduled** tab, select the job that you want to configure.

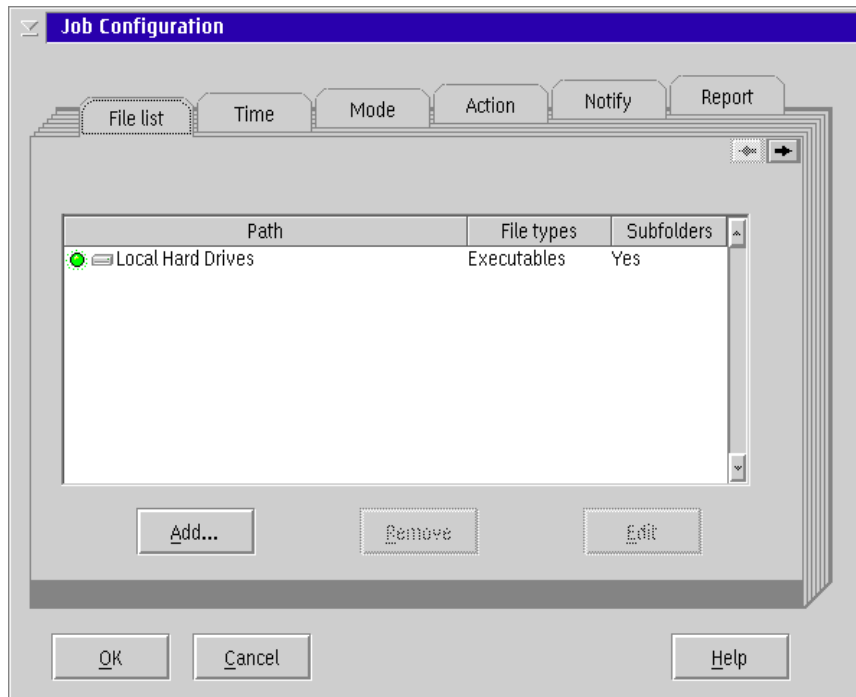
Then click the **Configuration** button.



The sub-sections in this section describe each tabbed page you will find in the configuration dialog boxes. Some tabbed pages are only available for scheduled scanning.

## 5.1 File list (scheduled mode only)

The **File list** tabbed page enables you to specify the items to be included in a scheduled scan. It is used in the same way as the file list on the **Immediate** tabbed page of the **Sophos Anti-Virus** window ([section 1.1.2](#)).



To add items to the list, click **Add** and specify an item or items in the item details dialog.

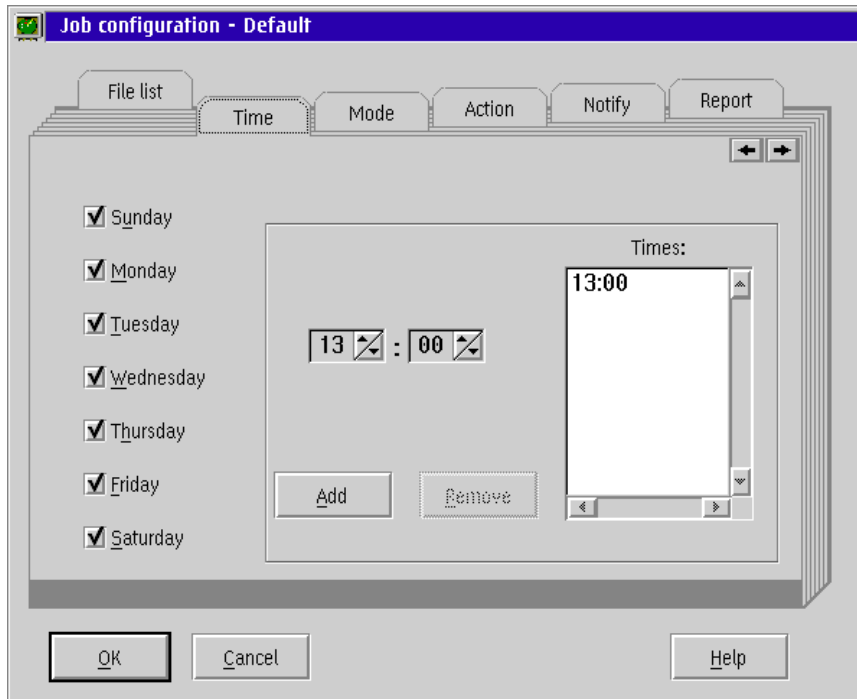
To remove an item, highlight it and click **Remove**.

To edit an item, double-click it, or highlight it and click **Edit**, then edit it in the **Edit item details** dialog box.

The options in the **Edit item details** dialog box are described in [section 1.2.2](#).

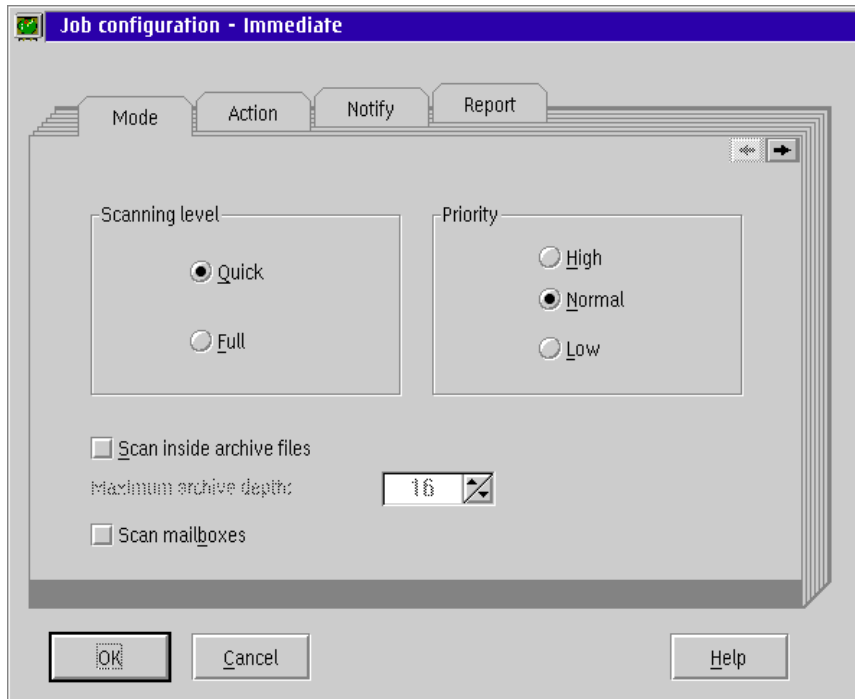
## 5.2 Time (scheduled mode only)

The **Time** tabbed page enables you to set the times and days on which a scheduled job should take place.



## 5.3 Mode

The **Mode** tabbed page enables you to configure scanning options for immediate or scheduled scans.



**Quick** scanning checks only those parts of each file that are likely to contain viruses. This level is sufficient for normal operation.

**Full** scanning examines the complete contents of each file. This level is more secure but is much slower than **Quick**.

- ❗ **Full scanning is needed in order to detect some viruses, but should only be enabled on a case-by-case basis (e.g. on advice from Sophos technical support).**

### Priority

**High** priority gives Sophos Anti-Virus precedence over any other applications.

**Normal** priority gives Sophos Anti-Virus the same priority as other applications.

**Low** priority reduces impact on system performance by ensuring that scanning only occurs when the system is otherwise idle.

### **Scan inside archive files**

Select this option if you want to scan inside archive files.

The archive types that can be checked include: ARJ, compress, gzip, LHA, Microsoft Compress, RAR, self-extractors, tar, UUEncode and Zip. See the readme file for the latest details. To enable Sophos Anti-Virus to scan inside only specific archive types, including Microsoft Cabinet files, see [section 7.11.4](#).

Sophos Anti-Virus can also scan archive files nested in archive files. Use **Maximum archive depth** to set the number of levels of nested files (between 0 and 32). The default is 16.

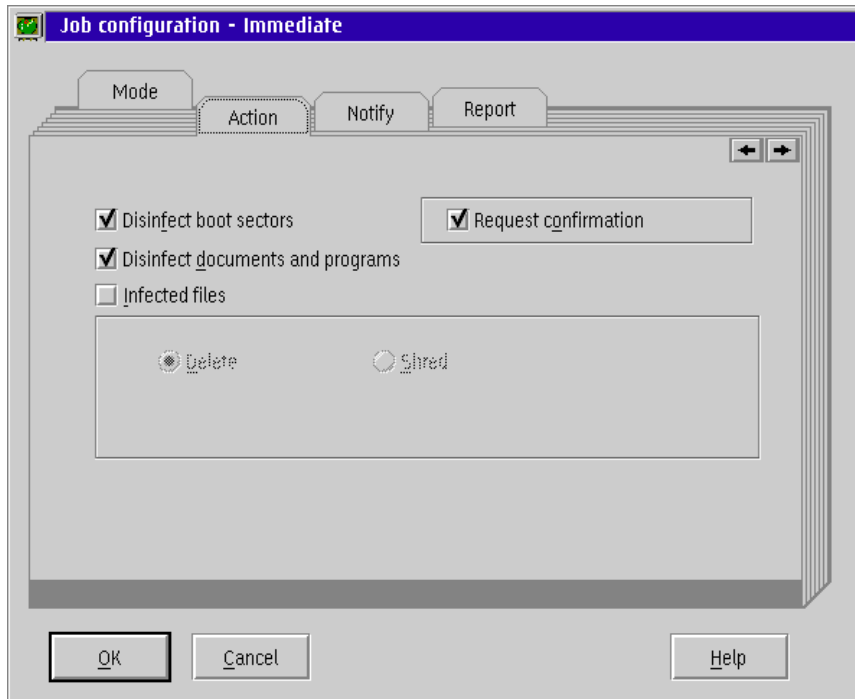
- ❗ Sophos Anti-Virus does not recognise archives nested to a greater depth than the maximum you specify and will not scan inside them.

### **Scan mailboxes**

Select this option if you want Sophos Anti-Virus to scan emails and attachments in Outlook Express mailboxes.

## 5.4 Action

The **Action** tabbed page enables you to specify the action immediate or scheduled scanning will take on finding a virus.



### Disinfect boot sectors

Sophos Anti-Virus can disinfect boot sectors on floppy and hard disks automatically. A hard disk cannot be disinfecting if any files on it are active. If disinfection of a hard disk fails, follow the instructions for disinfection in [section 4.2.1](#).

### Disinfect documents and programs

Sophos Anti-Virus can disinfect some programs and documents infected with most types of macro virus.

- ❗ **Check the contents of any disinfected documents carefully, as the virus may have corrupted them.**
- ❗ **Delete any disinfected programs and replace them from backups, as the virus may have corrupted them.**

### Infected files

If an infected file is found, it can be deleted or shredded automatically. Shredding is a secure type of file deletion that overwrites the file.

- ❗ **If you choose to delete or shred files, Sophos Anti-Virus does not attempt to disinfect them first, even if you select disinfection as well. However, Sophos Anti-Virus does not delete or shred infected mailboxes.**

#### **Request confirmation**

If this is selected, Sophos Anti-Virus will ask for confirmation before it does anything with infected items. The request is made before each immediate scan. This option is not available for scheduled scanning.

## 5.5 Notify

The **Notify** tabbed page enables you to configure the alerts sent on discovery of a virus.



To send alerts, Sophos Anti-Virus runs a batch file after each infected item is found, at the end of the job in which the viruses are found, or both. There are separate batch files for the two forms of notification.

To create these file(s), open a text editor and create a batch file.

The following parameters can be used in the first batch file (run after each infected item):

%1	machine name
%2	job name
%3	virus name
%4	location

The file NTFY.COM, used by InterCheck to report viruses, is suitable for use as the per-item batch file.

The following parameters can be used in the second batch file (run at the end of the job):

%1	machine name
%2	job name
%3	items (number of items scanned)
%4	viruses (number of viruses found)
%5	errors
%6	report file

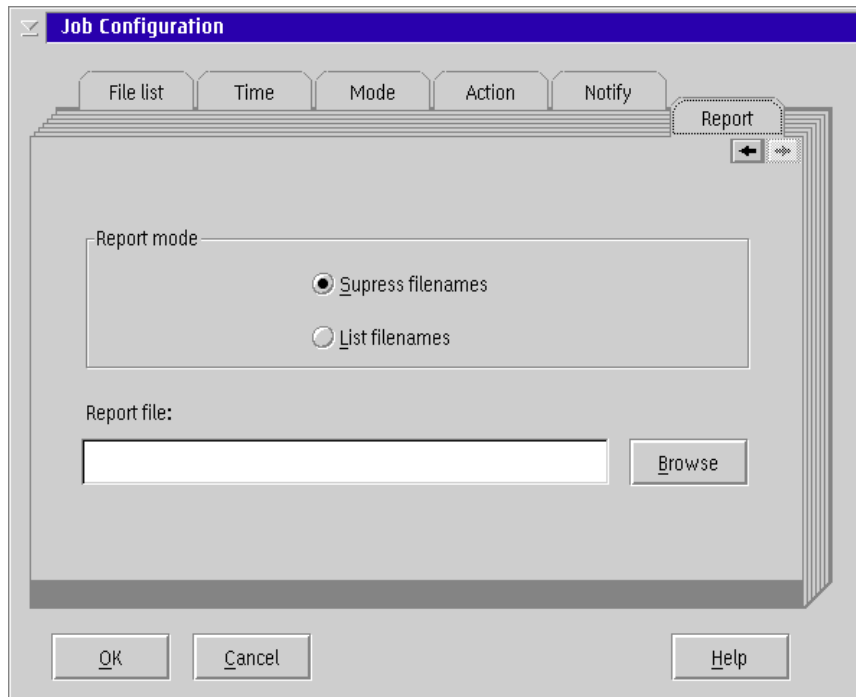
### **Notify timing**

The notification message can be a summary report sent at the end of each job and/or a message for every infected file found.

Use the browser to specify the batch file that will be run.

## 5.6 Report

The **Report** tabbed page enables you to configure the contents of the report file for each immediate or scheduled job. This file is generated in addition to the continuous log file.



### Report mode

Select **List filenames** to configure Sophos Anti-Virus to record in the report file the name of every item examined. By default, only infected items are recorded.

### Report file

Use this option to specify the location of the report file. This file is deleted and recreated each time a job is run.

## 5.7 Copying scheduled jobs to multiple computers on the network

If you have a central installation directory (CID) from which you installed the Sophos Anti-Virus GUI on OS/2 computers, you can set up scheduled jobs on one computer and copy them to all the other computers.

- ❗ So that any virus reports display the correct computer name, on each computer on the network, in the file CONFIG.SYS, add

```
SET HOSTNAME=xxx
```

where `xxx` is a computer-specific name. (If your OS/2 computers use IBM LAN Server or TCP/IP networking, or you set up central virus reporting (*Sophos Anti-Virus OS/2 computers on a network installation guide*), this should have been done already.) Restart each computer for this change to take effect.

1. At a computer where the Sophos Anti-Virus GUI is installed, open the **Sophos Anti-Virus** window.
2. Set up the required scheduled jobs. (For further configuration options, see [section 6](#).)
3. Close the **Sophos Anti-Virus** window.
4. Copy the file SWEEP.CFG from the installation directory on this computer, by default C:\SAV\OS2SWEEP\ENG, to the CID on the server, by default C:\SAVCID\OS2INST.
5. Change directory to the CID. Enter

```
SETUP -UPDATE
```

The server and the workstations detect the changes and are updated with the new configuration.

## 6 Global configuration options (GUI)

This section describes global configuration options accessible from the menu bar in the **Sophos Anti-Virus** window. It contains the following information:

- How to change the location of the Sophos Anti-Virus log folder (section 6.1).
- How to change the files defined as executables for all scanning modes (section 6.2).
- How to exclude files or file types from scanning by all scanning modes (section 6.3).
- How to set the machine name used by Sophos Anti-Virus alerts (section 6.4).
- How to clear the Sophos Anti-Virus log (section 6.5).
- How to set the web browser and language used to display virus analyses (section 6.6).
- How to disable the progress bar displayed during a scan (section 6.7).

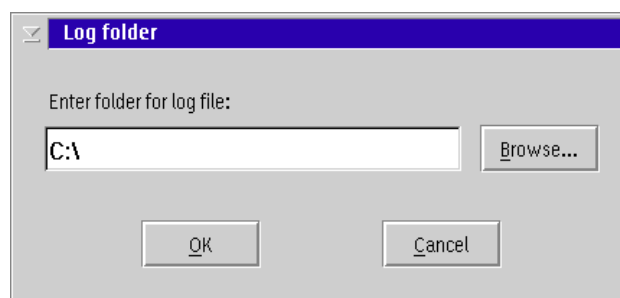
It also lists the Sophos Anti-Virus command line qualifiers (section 6.8).

### 6.1 Set log folder

Sophos Anti-Virus maintains a continuous log of all its activity. This log file contains administrative messages along with on-screen messages.

By default the log file is saved in the directory in which Sophos Anti-Virus was installed (the default is C:\SAV). This can be changed by clicking **Set Log Folder** on the **File** menu.

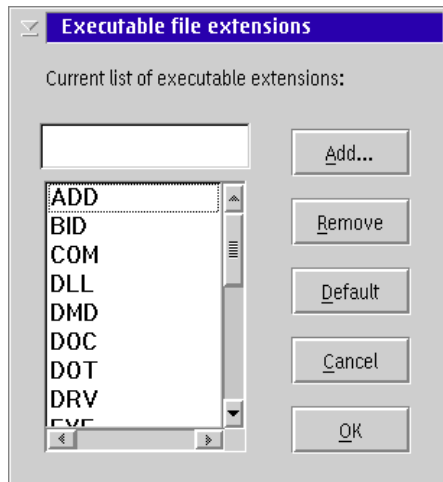
In the **Log Folder** dialog box, type in or browse to the path to the required log folder location.



## 6.2 Executables

To edit the list of filename extensions treated as executables, on the **Options** menu, click **Executables**.

Then specify extensions in the dialog box.



This list is used only if Sophos Anti-Virus is set to check executable rather than all file types. (Checking only executable types is the default.) See [section 1.2.2](#) to find out how to change this setting. The list does not apply to the command line interface or InterCheck.

- ❗ The list is automatically updated with filename extensions associated with new viruses, whenever you update Sophos Anti-Virus. If you edit the list as explained above, and you subsequently want to revert to the default list, click **Default**.

## 6.3 Exclusion list

The exclusion list is a list of specific files to be excluded from immediate and scheduled scanning. To edit it, on the **Options** menu, click **Exclusion List**.

Then add or remove items in the **Exclusion List** dialog box.

The list does not apply to the command line interface or InterCheck.

## 6.4 Machine name

If Sophos Anti-Virus is configured to notify other users of virus finds, it is useful to identify the computer where the virus has been found. To do this, on each computer on the network, in the file CONFIG.SYS, add

```
SET HOSTNAME=xxx
```

where xxx is a computer-specific name.

Restart each computer for this change to take effect. This method ensures all the components of Sophos Anti-Virus for OS/2 use the computer name.

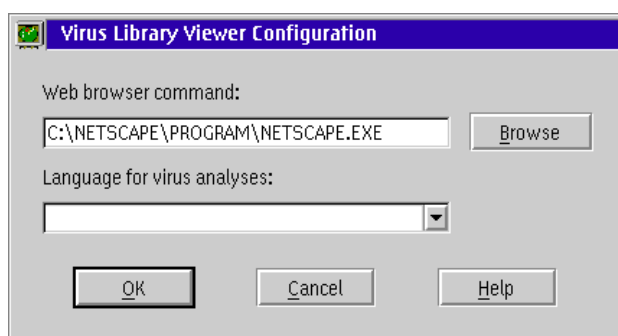
It is also possible to use the **Machine Name** option on the **Options** list to set the machine name. However, this only applies to virus finds reported by the GUI.

## 6.5 Clear log

The on-screen log provides a record of activity in the current session and reflects the information that is appended to the continuous log file. This option clears the on-screen log but does not affect the continuous log file on disk.

## 6.6 Virus library

To configure the web browser and language used to display the virus analyses on the Sophos website, on the **Options** menu, click **Virus Library** to display the **Virus Library Viewer Configuration** dialog box.



Choose the web browser by typing the path of the browser program in the **Web browser command** text box or by using the **Browse** button. The default is the computer's default browser, if one has been set. To use the OS/2 internet dial-up feature, precede the path of the browser program with 'linkup', for example

```
linkup C:\netscape\program\netscape.exe
```

- ❗ Do not choose the IBM Web Explorer browser, because it cannot display the Sophos web pages properly.

Choose the language by clicking the drop-down arrow on the **Language for virus analyses** box and selecting the appropriate language.

## 6.7 Progress bar

In order to display the progress bar, Sophos Anti-Virus has to count all the items to be scanned before starting the scan. On large network drives this can take a significant length of time, which can be saved by disabling this option. This will not affect any Sophos Anti-Virus jobs that are already running at the time the option is disabled.

- ❗ This option is set separately for immediate mode and each scheduled job.

## 6.8 Immediate and scheduled scan command line qualifiers

You can use the command SWEEP to start the Sophos Anti-Virus scan scheduler and to open the **Sophos Anti-Virus** window. When you use this command, certain command line qualifiers can be used to configure scanning and reporting.

Either '-' or '/' can be used when entering a qualifier, i.e. /AUTO and -AUTO are identical.

### **-AUTO**

Starts scanning when the **Sophos Anti-Virus** window is opened, using the most recent configuration set at the **Immediate** tabbed page.

### **-EXEJOB <jobname>**

Starts the scheduled job named <jobname> when the **Sophos Anti-Virus** window is opened instead of waiting until the scheduled time.

The -EXEJOB and -AUTO qualifiers cannot both be used; if both are included in the command line, -EXEJOB will be ignored.

### **-CLOSE**

Closes both the **Sophos Anti-Virus** window and the background scheduler.

If Sophos Anti-Virus is not running, errorlevel 1 is returned. All other qualifiers are ignored.

**-CF <config file>**

Specifies a name and path for the configuration file.

If the program cannot open the file, Sophos Anti-Virus will be started with default options, and on exit will try to create a configuration file with the given path and filename.

**-NOWIN**

Starts the background scheduler only.

**-LOGPATH <path>**

Enables the user to alter the stored (or default) location of the log file, SWEEP.LOG. The new path will be stored in the configuration file.

**-REPORTPATH <path>**

Enables the user to enter a default path for the (job) report files. This path will be used when no path is entered for a report file in the appropriate dialog.

## 7 Configuration via the CLI

This section describes how to configure Sophos Anti-Virus from the command line or with an area file. It describes how to:

- specify which items should be scanned (sections 7.1 to 7.5)
- specify full or quick scanning (section 7.6)
- run scanning at different priorities (section 7.7)
- use new virus identities or patterns (sections 7.8 and 7.9)
- disinfect or remove files (section 7.10).

It also lists all the Sophos Anti-Virus command line qualifiers and error codes (sections 7.11 and 7.12).

 For information on default settings, see [section 2.1](#).

### 7.1 Specifying what Sophos Anti-Virus will check

Users can specify which items will be scanned using either

- the command line, or
- an area file, SWEEP.ARE.

The command line enables the user to specify drives, directories, files or drive sectors. It can also include the command line qualifiers listed in this section.

The SWEEP.ARE file enables the user to specify what will be scanned in greater detail, down to the level of a byte or group of bytes.

### 7.2 Specifying items to be checked in the command line


Items to be checked can be specified in the command line. For example, to check the file ISVIRUS.BIN type

```
OSWEEP ISVIRUS.BIN
```

or to check all executable files on drives D: and E: type

```
OSWEEP D: E:
```

Make sure that any symbols used do not conflict with the OS/2 meaning. For example, do not use the recursion symbol '>' in the command line, as it means redirection in OS/2.

 When the items to be checked are specified, all default settings will be overridden unless the -AS qualifier is added to the command line.

## 7.3 Specifying items to be checked in SWEEPARE

Items to be checked can be specified in an area file, SWEEPARE. This must reside in the current drive and subdirectory. For example, if the current drive and directory is C:\PROGS, SWEEPARE must reside on the C: drive in the directory C:\PROGS.

- When the items to be scanned are specified, all default settings will be overridden unless the -AS qualifier is added to the command line.

The SWEEPARE file can be edited as required. The syntax for describing areas to be checked is given in the following sections. For example, SWEEPARE may contain

```
D: | 0
D: > * .EXE
D: > * .OVL
+81 0 0 1
```

which will check the boot sector on drive D:, all EXE and OVL files on drive D: and physical sector 1 on the second hard disk.

- The | symbol is the OS/2 pipe operator and is not the same as 1 (one) or l (letter l).

Drives can also be specified in the command line. For example, to check drives A: and D: while Sophos Anti-Virus is on drive C:, type

```
OSWEEP A: D:
```

Note that a default drive can precede any areas defined in the SWEEPARE file which do not already specify a drive. For example, if SWEEPARE contains

```
* . *
D: | 0
```

and the user issues the command (see -AD command line qualifier for a full explanation)

```
OSWEEP -AD=A
```

then SWEEP will check

```
A: * . *
D: | 0
```

## 7.4 Specifying files to be checked in SWEEP.ARE

Particular file types and areas can be specified in SWEEP.ARE using the normal OS/2 descriptions. For example

```
C:\*.ABC
```

makes Sophos Anti-Virus examine all files with extension .ABC in the root directory of drive C:.

The recursion operator '>' can be used to specify that all subdirectories, as well as the current directory, should be searched. For example, if the entry

```
C:* .ABC
```

is specified, and the disk in drive C: contains two subdirectories, **only the current directory** will be searched for ABC files. On the other hand, if the entry

```
C:>* .ABC
```

is specified, not only the current directory but also both subdirectories will be searched for ABC files. Similarly, if the entry

```
C:\MYAREA\MYFILES\>* .ABC
```

is specified, the search will cover the subdirectory C:\MYAREA\MYFILES and all its child directories.

Remember that the more files specified, the longer it will take to check the system.

To check all executable files (COM, EXE, OV?, SYS, DLL, DRV, IFS, etc) specify

```
C:"All executables"
```

Sweeping is about 30% faster than when each group is specified individually. The drive specification (C: in above example) is optional.

### Excluding files from checking

Certain files or directories can be excluded from checking, by preceding the description with the '<' exclusion operator. For example

```
C:\>* .EXE
```

```
<C:\DONOT.EXE ; will not be examined
```

will recursively search all EXE files except DONOT.EXE in the root directory of drive C:. If the name of a file **without a drive or path** is specified, all files or directories with that name will be excluded.

For example

```
<FOO.EXE
; file FOO.EXE will be excluded
; in whatever drive and
; directory it may appear
<C:FOO.EXE
; FOO.EXE will be excluded in
; the current directory of
; drive C
<\J\FOO.EXE
; FOO.EXE will be excluded if
; found in the \J directory of
; the current drive
<J\FOO.EXE
; FOO.EXE will be excluded if
; found in the J subdirectory
; of the current directory on
; the current drive
```

- ❗ Wildcard characters cannot be used with the exclusion operator.

Any exclusion descriptors which contain the '\' symbol and do not specify a drive will have the drive specified in the -AD command line qualifier inserted. For example, if SWEEP.ARE contains

```
<\NU.EXE
```

and Sophos Anti-Virus is started with the command line qualifier

```
OSWEEP -AD=C:
```

the file which will be excluded will be C:\NU.EXE. This is equivalent to entering

```
<C:\NU.EXE
```

in the SWEEP.ARE file.

## 7.5 Specifying disk sectors to be checked in SWEEP.ARE

At a lower level than the file structure, disks are organised into sectors. The most important of these are the master boot sector and the partition boot sector, as they contain executable program code which many viruses attack. A floppy disk has only a partition boot sector.

Sectors can be referred to in two different ways: as logical sectors or as absolute sectors. A logical sector number refers to the position of the sector

within a particular drive or partition. This is useful when referring to the partition boot sector, which is logical sector 0 of the partition. The absolute specification of a sector is in terms of the cylinder, head and sector of its physical position on the specified device. While more complex than a logical sector number, it allows any sector on the disk to be specified. This is important for checking the master boot sector, which can be found at cylinder 0, head 0, sector 1. On hard disks this sector is not accessible using a logical sector number. On floppy disks, absolute sector 0,0,1 and logical sector 0 are the same physical sector.

### **Specifying logical sectors to be checked**

To specify a particular logical sector or set of sectors, use the '|' symbol (the OS/2 pipe operator). It is also possible to specify a byte or group of bytes to be checked in each sector (for example if the sector contains variable information). The format of the specification is

```
drive | ssector esector sbyte ebyte
```

where

- drive is the drive letter, e.g. C: (optional)
- ssector is the first logical sector to be checked
- esector is the last logical sector to be checked (optional)
- sbyte is the first byte to be checked (optional)
- ebyte is the last byte to be checked (optional).

All values must be in decimal format.

For example

```
C: | 0
```

specifies that the whole of logical sector 0 on drive C: should be checked, whereas

```
C: | 0 10
```

specifies that a check should be taken of logical sectors 0 to 10 inclusive, and

```
C: | 0 10 271 275
```

specifies further that in each of the logical sectors 0 to 10, only bytes 271 to 275 inclusive should be checked.

The following specification would check logical sector 15 on drive A:, checking only byte number 536 within that sector:

```
A: |15 15 536
```

The start- and end-sectors have been specified the same.

In addition, the following can be used on all drives except network drives

```
| *
```

This checks all disk sectors within the current logical disk, and should be used with care, because it might find virus fragments in deleted files, and might cause false positives.

### **Specifying absolute sectors to be checked**

To specify an absolute sector, use the '+' symbol followed by the drive number, the cylinder (or 'track') number, the head (or 'side') number and the sector number within that cylinder. The first floppy disk drive in the system is number 0, the second is number 1, and so on. The first physical hard disk drive is number 80, the second is number 81 and so on. It is also possible to specify a byte or group of bytes to be checked in the sector (for example if the sector contains variable information).

The format of the specification is

```
+drive cylinder head sector sbyte ebyte
```

where

- drive is the disk drive number
- cylinder is the cylinder number
- head is the head number
- sector is the sector number
- sbyte is the first byte to be checked (optional)
- ebyte is the last byte to be checked (optional).

All values must be in hexadecimal format.

For example

```
+80 0 0 1
```

specifies that sector 1 of cylinder 0, head 0 on the first fixed disk (usually drive C:) should be checked, whereas

```
+1 0 0 1 23 1B7
```

specifies that a check should be taken of bytes 23 hex to 1B7 hex inclusive on sector 1 of cylinder 0, head 0 on the second floppy-disk drive (usually drive B:).

To check master boot sectors on drives 80 to 83 Hex, specify

```
C:"All master boot sectors"
```

If a particular drive is not present, no error message is produced.

## 7.6 Full and quick scanning

**Quick** scanning checks only those parts of each file that are likely to contain viruses. This is the default setting and is sufficient for normal operation.

**Full** scanning examines the complete contents of each file. This level is more secure but is much slower than **Quick**.

- ❗ **Full scanning is needed in order to detect some viruses, but should only be enabled on a case-by-case basis (e.g. on advice from Sophos technical support).**

A full scan can be selected with the command line qualifier **-F**. See section 7.11.3.

## 7.7 Running Sophos Anti-Virus at different priorities

When a scan is run, it is scheduled by OS/2 to run with the same priority as any other OS/2 application, such as a word processor. Network servers run at a high priority in order to achieve rapid response.

Sophos Anti-Virus should be run in high priority mode if a virus is suspected on your system and the user wishes to run the scan as soon as possible and as fast as possible, without shutting the system down. Use the command line qualifier **-PR=H**.

```
OSWEEP -PR=H
```

Sophos Anti-Virus will run with the same high priority as the network software, but at a lower priority than any real-time processes.

Scanning should be run in low priority (lower than any other task) if the user wishes to check constantly for virus presence, without affecting the system performance. Use the command line qualifier `-PR=L`.

```
OSWEEP -PR=L
```

This makes Sophos Anti-Virus run only when OS/2 would otherwise be idle.

## 7.8 Scanning with new virus identity files

See the *Sophos Anti-Virus OS/2 computers on a network installation guide* or the *Sophos Anti-Virus OS/2 single user installation guide* for information about updating Sophos Anti-Virus with new virus identity files (IDEs). To specify the location of the IDEs that Sophos Anti-Virus should use, use the command line qualifier `-IDEDIR` (section 7.11.3).

## 7.9 Scanning with new patterns

The range of patterns checked by Sophos Anti-Virus can be extended by creating a file called `SWEEP.PAT` containing the patterns in the format

```
Name Hex1 Hex2 ... Hexn ; Comments
```

where

- Name is the pattern name (no spaces allowed)
- Hex1 etc are pattern bytes in hexadecimal, 2 hex digits per byte, most significant nibble first
- ; Comments are any comments after the ‘;’

Pattern bytes can be separated by spaces or tabs. A name can contain up to 15 characters and a pattern can be up to 24 bytes long.

If the line starts with a space or a tab, the pattern will have the name ‘Noname n’ where n is a number from 0 upwards.

For example, `SWEEP.PAT` may contain

```
ABC_Virus 26 83 88 9c 9f f9 f0 23
```

```
HAL_Virus ABCDEF0123456789 ; comment
```

- ❗ **SWEEP.PAT must reside in the current drive and subdirectory.** For example, if the current drive and directory is `C:\PROGS` and drive A: is being checked using the command

```
OSWEEP A:
```

then `SWEEP.PAT` must reside on the C: drive in the directory `C:\PROGS`.

- ❗ Sophos Anti-Virus looks for patterns only when it is run in full scanning mode (quick is the default). The -F qualifier must be specified. For example

```
OSWEEP C: -F
```

## 7.10 Virus disinfection and removal

Common boot sector viruses can be removed from hard and floppy disks, and macro viruses from documents, by using Sophos Anti-Virus's built-in disinfection capability. To do this, run OSWEEP with the command line qualifier -DI.

Sophos Anti-Virus can also be used to delete infected programs while the system is running. This is done with the -REMOVEF qualifier.

See also [section 4](#).

## 7.11 Sophos Anti-Virus command line qualifiers

When you use the command OSWEEP, certain command line qualifiers can be used to control and/or automate the scanning process. The qualifiers are described in the following subsections, or can be listed using

```
OSWEEP -?
```

The command format is

```
OSWEEP drive file1 ... filen qual1 ... quan
```

where

- drive is the optional drive which will be checked (A:, B:, C: etc) and '\*' denotes all local hard drives
- file1 to filen are optional descriptors of files checked
- qual1 to quan are optional command line qualifiers (all beginning with either a hyphen '-' or a slash '/')

The **order** of the items after OSWEEP is unimportant, except for the qualifiers for archive types (see [section 7.11.4](#)).

For example

```
OSWEEP A:
```

scans the floppy disk in drive A: while

```
OSWEEP -P=ALL.LOG -NS
```

scans all local hard disks, listing each file in the file ALL.LOG.

### 7.11.1 @file Command line qualifiers from an external file

Sophos Anti-Virus can obtain its command line qualifiers from an external text file. For example

```
OSWEEP @SWEEP.CM E:
```

when the file SWEEP.CM contains

```
-NS -NK
C: D:
-P=SWEEP.LOG
```

is equivalent to

```
OSWEEP -NS -NK C: D: -P=SWEEP.LOG E:
```

- ❗ Command files can contain any number of items per line (up to the maximum number of characters permitted per line).

### 7.11.2 Command files compared with .ARE files

Both .ARE files and command files can contain the symbols '<' (exclusion), '>' (subdirectory recursion) and '|' (logical sector specification).

.ARE files contain exactly one item per line; command files can contain any reasonable number.

Command files can contain qualifiers (-NS, -NK etc); .ARE files cannot.

.ARE files can contain specifications containing spaces, e.g. +80 0 0 1, 'All executables', and comments; command files cannot.

### 7.11.3 List of command line qualifiers to OSWEEP

#### -? Help

Sophos Anti-Virus displays all command line qualifiers and a short description of their function.

#### -A Append report

By default, any security report written to a file by Sophos Anti-Virus will be overwritten by a subsequent report written to a file of the same name. Specifying the -A qualifier in the command line, for example

```
OSWEEP -A -P=FOO.REP
```

appends the new report to the old file FOO.REP, rather than overwriting the old report with the new one.

If this is used in an automatic process, this file should be pruned from time to time to stop it taking up ever more disk space, especially if the -NS command line qualifier is used.

#### **-AD= <drive> Area file default**

Any files or areas listed in the SWEEP.ARE file are assumed to be in the specified drive, unless they have an explicitly stated drive.

For example

```
OSWEEP -AD=X
```

would assume that all areas refer to drive X.

#### **-AF= <filename> Area file**

The default area file is called SWEEP.ARE. The -AF qualifier can be used to specify a different name.

See also [section 7.3](#).

#### **-ALL Scan all files**

In order to scan all files on a disk instead of just the executable files, specify the -ALL command line qualifier. This is equivalent to creating a SWEEP.ARE file which contains


```
\>*. *
```

It thus specifies a recursive search of all files (rather than just executable files) from the root directory of the current drive.

For example

```
OSWEEP A: -ALL
```

will recursively sweep all files on drive A:.

 This is a slow process.

#### **-ARCH[=n] Scan inside archive files**

This qualifier enables Sophos Anti-Virus to scan inside archive files. The archive types scanned include ARJ, compress, gzip, LHA, Microsoft Compress, RAR, self-extractors, tar, UUEncode and Zip. See the readme file for the latest details. To enable Sophos Anti-Virus to scan inside only specific archive types, including Microsoft Cabinet files, see [section 7.11.4](#).

By default, Sophos Anti-Virus will unpack 16 levels of nested archive files (i.e. archive files within archive files). If you want to change this setting, use

-ARCH=n, where n is the maximum number of levels. The number n can be between 0 and 32.

### **-AS Scan standard areas**

If an area to be scanned is specified in the command line, Sophos Anti-Virus will not scan standard areas (master boot sector, OS/2 boot sector etc). With the -AS command line qualifier, standard areas are checked as well.

For example

```
OSWEEP SUSPFILE.EXE -AS
```

will scan SUSPFILE.EXE as well as the standard areas.

### **-CDR Scan CD boot image**

To scan the boot image of a CD, use the -CDR qualifier. For example

```
OSWEEP -CDR H:
```

scans all executables, logical sector 0 and the boot image (if any) of CD drive H:. If Sophos Anti-Virus finds a boot image, it checks the boot sector of that image for boot sector viruses, and scans all executables in the boot image for file viruses.

### **-CI Check integrity**

This qualifier causes Sophos Anti-Virus to check the integrity of OSWEEP.EXE before executing. A change in the contents of OSWEEP.EXE may indicate the presence of a virus or some other form of data corruption.

### **-D=<day|percentage> Day or Percentage**

Sophos Anti-Virus may be incorporated into the STARTUPCMD file; however it may not be desirable to perform the system check every time the computer is switched on. The -D qualifier enables you to specify either the probability with which SWEEP will actually proceed to check the system, or the day of the week on which the system should be checked.

For example

```
OSWEEP -D=MONDAY
```

will only run Sophos Anti-Virus when invoked on a Monday. The day of the week can be abbreviated to a minimum of two letters (e.g. MO for Monday, TU for Tuesday, etc).

Alternatively

```
OSWEEP -D=20
```

makes Sophos Anti-Virus check the system on average 20 times out of every 100 times that SWEEP is invoked. The number specified must be an integer between 0 and 100.

See also the -DE qualifier.

### **-DA Display areas**

This command line qualifier will list all areas to be checked by Sophos Anti-Virus, but not actually check them.

### **-DE Daily execution**

This command line qualifier will check whether Sophos Anti-Virus has already been executed that day and if it has, it will not be executed again.

The file SWEEP.DAY is created on the current drive and directory.

A different file can be specified by including '=filename' after the -DE qualifier. For example

```
OSWEEP -DE=SWEEP.DA1
```

### **-DI Disinfect**

This qualifier enables Sophos Anti-Virus to perform automatic disinfection of some boot sector, macro and file viruses. For more information on using it, see [section 4](#).

**!** **Boot sector virus disinfection will not work if the boot sector has already been disabled by using the -REMOVE qualifier.**

### **-DIB**

Use the -DIB qualifier to disinfect only boot sectors.

### **-DID**

Use the -DID qualifier to disinfect only documents and programs.

### **-DN Display names of files as they are scanned**

The display consists of the time followed by the item being scanned.

### **-EEC Use extended set of error codes**

This qualifier directs Sophos Anti-Virus to use an extended set of error codes. For details, see [section 7.12](#).

**-EX= <extensions> Executable extensions**

The extensions of files normally treated as executables can be changed with the -EX command line qualifier.

For example

```
OSWEEP -EX=EX1,EX2
```

replaces the list of extensions with the EX1 and EX2 file types.

**-F Full SWEEP**

By default, Sophos Anti-Virus checks only those parts of each file likely to contain viruses. A full scan examines the complete contents of each file and can be specified by using this qualifier. Note that a full scan is much slower than a quick scan. See also [section 7.6](#).

**-FM Specify message file**

Sophos Anti-Virus will output the contents of the file specified with this qualifier to the screen if it discovers one or more viruses. This facility can be used to customise virus recovery procedures. You must specify the full path to the file. The default filename of the message file is SWEEP.MSG.

For example

```
OSWEEP -FM=C:\MY_MSG.TXT
```

specifies the file 'MY\_MSG.TXT' in the root directory of drive C:.

**-FS File server**

Use the -FS qualifier if checking a file server over a network. This qualifier prevents checking of the boot sectors (which most networks do not allow). See also [section 2.4](#).

**-IDEDIR= <directory> Use alternative directory for virus identity files**

This qualifier enables you to specify an alternative directory for IDEs. For example

```
OSWEEP -IDEDIR=C:\IDE
```

directs Sophos Anti-Virus to read IDEs from the C:\IDE directory instead of the default directory (C:\SAV\OS2SWEEP\ENG).

If Sophos Anti-Virus is reading the main virus data (VDL.DAT) and IDEs from the same floppy disk drive, the IDEs must be on the final virus data disk (the disk containing VDL.D03).

### **-MIME Scan MIME files**

This qualifier enables Sophos Anti-Virus to scan MIME files when it does a scan. By default, it is *not* enabled to scan MIME files.

### **-MU Check multiple disks**

This command line qualifier enables the user to check a succession of disks in a drive without reloading SWEEP.EXE every time.

For example, to check multiple disks in drive A: type

```
OSWEEP -MU A:
```

When prompted, insert a disk in drive A: and press any key to start checking it. Once that disk has been checked, insert another disk into drive A: when prompted, and press any key to start checking. This will continue until 'Esc' is pressed to interrupt the checking, or one or more viruses are detected.

### **-NAF Do not read file with areas to be checked**

By default, Sophos Anti-Virus will try to open the file SWEEP.ARE and read from it the names of any areas to be checked. Use this qualifier if it is not necessary to check the areas defined in SWEEP.ARE.

### **-NAS Do not check standard areas**

By default, Sophos Anti-Virus will check standard areas defined at compile time. Use this qualifier to prevent these areas from being checked (for example, if the areas to be checked have been specified in SWEEP.ARE).

 SWEEP.ARE must reside on the current drive and in the current subdirectory.

### **-NB No bell**

When a virus is discovered, Sophos Anti-Virus sounds a bell. This can be disabled using the -NB qualifier.

### **-NDI Do not disinfect infected items**

Cancel -DI.

### **-NE Do not use the emulator**

Sophos Anti-Virus finds various polymorphic viruses by emulating the environment in which the virus code would normally execute, making the virus decrypt and reveal itself. Disabling this emulator will speed up a scan, but may result in some polymorphic viruses not being found.

**-NI No interrupting**

Execution of a scan can normally be interrupted by pressing 'Esc' or 'Ctrl' + 'Break'. If this command line qualifier is used, execution cannot be interrupted.

**-NK No key to continue**

If Sophos Anti-Virus discovers one or more viruses or virus fragments, it pauses at the end of the security report and asks for a key to be pressed before continuing. To skip this, use the command line qualifier -NK.

**-NMIME Do not scan MIME files**

Cancels -MIME.

**-NOC No confirmation before virus removal**

If this qualifier is used, Sophos Anti-Virus does not ask for confirmation before deleting an infected file or disabling an infected boot sector.

This qualifier has no effect unless -REMOVE is also specified.

 **Use this qualifier with care.**

**-NOE Do not scan Outlook Express mailboxes**

Cancels -OE.

 This qualifier does *not* disable scanning of MIME files.

**-NP Do not display full pathname**

If Sophos Anti-Virus has been set to display the names of the areas it checks, it normally displays the full path of the files (see the -NS qualifier). Using the -NP qualifier means only the names of the files it checks are recorded.

 This also affects the information placed in the security report created by the -P qualifier.

**-NS Not silent**

Using this command line qualifier causes the name of each area to be displayed as it is scanned. Files within archive files are flagged by default with a variable length arrow symbol. To change this listing, use one of the following:

-NS=F	Do not list files within archive files at all. List only the names of the outermost archive files that appear in the OS/2 file system.
-NS=P	Flag files within archive files with arrow symbol (default).
-NS=U	List the full paths of all files within archive files. Include the names of archive files, including those inside other archive files, in these paths as though they are directories.

If this qualifier is omitted, only **infected** archives are listed, using the same format as -NS=U.

### **-NSSA Scan files that Sophos Anti-Virus incorrectly identifies as “zip bombs”**

By default, Sophos Anti-Virus stops scanning “zip bombs” when they are detected.

- ❓ “Zip bombs” are malicious files that are designed to disrupt the action of anti-virus scanners. These files usually take the form of innocent looking archive files that, when unpacked in order to be scanned, require enormous amounts of time, disk space, or memory.

When a “zip bomb” is detected, a message such as

```
Aborted scanning of C:\TEMP\BOMB.ZIP - appears to be a "zip bomb"
```

is displayed. Occasionally, Sophos Anti-Virus incorrectly identifies files that have complex and/or multiple levels of archiving as “zip bombs”, and stops scanning them. To scan such files, rescan them using the qualifier -NSSA. For example

```
OSWEEP C:\TEMP\PACKAGE.ZIP -NSSA
```

directs Sophos Anti-Virus to scan package.zip, even if it identifies it as a “zip bomb”.

- ❗ Use this qualifier only if absolutely necessary. If a genuine “zip bomb” is accessed with this qualifier, Sophos Anti-Virus continues to scan it.

Users of the Sophos Anti-Virus for OS/2 GUI can make use of this feature by entering the -NSSA qualifier as an advanced option (on the **Options** menu, click **Advanced Options**).

### **-NTW No Temp Warning**

Sophos Anti-Virus performs a check to ensure the TEMP or TMP environment variable specifies a valid path to which it can write temporary files. A warning is issued if this check fails. The -NTW qualifier disables the check.

### **-NVOL Do not log the volume IDS of scanned disks**

If this qualifier is used, Sophos Anti-Virus does not log the volume IDS of disks that are scanned.

### **-OE Scan Outlook Express mailboxes**

This qualifier enables Sophos Anti-Virus to scan Outlook Express mailboxes and MIME files when it does a scan. By default, it is *not* enabled to scan Outlook Express mailboxes and MIME files.

### **-P[= <file|device>] Print security report**

This command line qualifier directs Sophos Anti-Virus to produce a report of the areas checked. This report is output to the device PRN, if the qualifier is used as -P (not followed by =).

Alternatively, the report can be directed to a particular file or device using the qualifier as -P=. For example

```
OSWEEP -P=SEC.DOC
```

directs Sophos Anti-Virus to write its security report to the file SEC.DOC.

### **-PD Pause on discovery of a match**

Sophos Anti-Virus will pause whenever it discovers a matching pattern and wait for a keystroke before continuing, if this command line qualifier is used.

### **-PR Priority**

By default, Sophos Anti-Virus runs with the priority of any other standard OS/2 task such as a word processor. This qualifier can be used to increase or decrease this priority.

```
OSWEEP -PR=H
```

specifies high priority, while

```
OSWEEP -PR=L
```

specifies low priority.

High priority is a little below that of real-time tasks, while low priority is equivalent to idle-time priority.

### **-Q Quick sweep**

By default, Sophos Anti-Virus performs a quick scan. This qualifier is only necessary if default mode is switched off. This might have been done, for example, in a batch file or in a file specified by @file.

### **-REC Recursive search**

This qualifier directs Sophos Anti-Virus to search directories below the ones specified in the command line. For example

```
OSWEEP C:\*.DLL C:\SIMULATI\*.SYM -REC
```

searches all .DLL files on the disk starting from the root directory (\) as well as all .SYM files from the \SIMULATI directory downwards.

### **-REMOVE Remove viruses on discovery**

This qualifier directs Sophos Anti-Virus to delete infected files and disable infected boot sectors.

The -RS command line qualifier can be used in conjunction with -REMOVE to ensure that the file is positively overwritten rather than simply deleted.

Confirmation will be requested before any item is deleted or disabled unless the -NOC qualifier is also used.

- ❗ **If you choose to delete or positively overwrite files, Sophos Anti-Virus does not attempt to disinfect them first, even if you use a disinfection qualifier as well. However, Sophos Anti-Virus does not delete or positively overwrite infected mailboxes.**

Disabling of boot sectors is done by substituting the first two bytes pointed to by the initial JMP instruction with a JMP-to-itself instruction. Afterwards, the virus fragment may still be there, but the virus will be inactive. For example

```
OSWEEP -REMOVE -RS -NOC
```

See [section 4](#).

### **-REMOVEF Remove infected files**

As -REMOVE, except that infected boot sectors are not disabled. For example

```
OSWEEP -REMOVEF
```

This is especially useful if it is inconvenient to boot OS/2 from floppy disk.

See [section 4](#).


**-RS Remove viruses by positively overwriting them**

Infected files will be positively overwritten instead of being deleted, if this qualifier is used.

Disabling of boot sectors is not affected.

-RS has no effect unless -REMOVE or -REMOVEF is also specified. For example

```
OSWEEP -REMOVE -RS
```

 Files overwritten when this qualifier is used cannot be recovered.

See [section 4](#).

**-S Silent running without displaying checked areas**

By default, Sophos Anti-Virus does not display on the screen the areas it is checking. The qualifier -S is equivalent to this default mode, and is the opposite of the -NS qualifier.

**-SC Scan inside compressed files**

By default, Sophos Anti-Virus looks for viruses inside files compressed by using dynamic compression utilities PKLite, LZEXE and Diet.

This qualifier is the equivalent of the default.

**-SS Super silent running**

Sophos Anti-Virus will not display anything (not even the copyright message) unless a virus is found, if this qualifier is used.

**7.11.4 Command line qualifiers for specific archive types**

By default, Sophos Anti-Virus does not scan inside the archive types in the following table. To enable Sophos Anti-Virus to scan inside a specific archive type, use the appropriate qualifier.

To enable Sophos Anti-Virus to scan inside all the archive types in the table except Microsoft Cabinet and InstallShield Cabinet files, use the [-ARCH](#) qualifier instead (section 7.11.3). You can also use this with the specific archive type qualifiers to more easily specify which archive types should be scanned. In this case, the qualifiers are processed from left to right. For example

```
OSWEEP -ARCH -NZIP
```

directs Sophos Anti-Virus to scan inside **all archive types except Zip** when it does a scan.

OSWEEP -NZIP -ARCH


directs Sophos Anti-Virus to scan inside **all archive types** when it does a scan.

Archive type	Filename extensions	Qualifier to <i>enable</i> scanning	Qualifier to <i>disable</i> scanning
ARJ	ARJ	-ARJ	-NARJ
bzip2	BZ2, TBZ, TBZ2	-BZIP2	-NBZIP2
compress	TAZ, Z	-CMZ	-NCMZ
gzip	GZ, TGZ	-GZIP	-NGZIP
InstallShield Cabinet	CAB	-ISCAB	-NISCAB
ITSS (compressed help)	CHM, HXS	-ITSS	-NITSS
LHA	LHA, LZH	-LHA	-NLHA
Microsoft Cabinet	CAB	-CAB	-NCAB
Microsoft Compress	??_	-MSCMP	-NMSCMP
RAR	RAR	-RAR	-NRAR
RPM	RPM	-RPM	-NRPM
Self-extractors	EXE	-SFX	-NSFX
tar	TAR	-TAR	-NTAR
Unix archives	A	-UAR	-NUAR
UUEncode	UUE	-UUE	-NUUE
Zip	ZIP	-ZIP	-NZIP

## 7.12 Error codes returned by SWEEP

Sophos Anti-Virus returns error codes that can be tested by using the IF ERRORLEVEL command in batch files. This enables automatic action to be taken if Sophos Anti-Virus discovers an abnormal condition.

- 0 If no errors are encountered and no viruses found.
- 1 If the user interrupts the execution by pressing 'Esc'.
- 2 If a corrupt or password-protected file is encountered, or if some error preventing further execution is discovered.
- 3 If viruses or virus fragments are discovered.

 These return values can be tested by using the IF ERRORLEVEL command. For example

```
@ECHO OFF
OSWEEP -NK
IF ERRORLEVEL 3 GOTO FISHY
IF ERRORLEVEL 1 GOTO SOMEERR
ECHO No problems
GOTO END
:SOMEERR
ECHO Some error has occurred
GOTO END
:FISHY
ECHO Something has been discovered
:END
```

This batch file will print

Something has been discovered

if Sophos Anti-Virus discovers a virus,

Some error has occurred

in the event of an error, or

No problems

if nothing is discovered. The -NK qualifier tells Sophos Anti-Virus not to pause for a key if viruses are discovered.

### Extended error codes

A different set of error codes are returned if Sophos Anti-Virus is run with the -EEC command line qualifier.

- 0 No errors have occurred and no viruses have been found.
- 8 Survivable errors have occurred.
- 16 Password-protected files have been found. (They are not scanned.)
- 20 Viruses have been found and disinfected.
- 24 Viruses have been found and not disinfected.
- 32 OSWEEP has failed an integrity check.
- 36 Unsurvivable errors have occurred.
- 40 Execution has been interrupted.

## 8 Configuring InterCheck

This section describes how to configure InterCheck on-access scanning and lists the options that you can set.

### 8.1 How to configure InterCheck

InterCheck is configured via the file INTERCHK.CFG, located on the workstations, in the same directory as Sophos Anti-Virus and InterCheck.

If the workstations have been set to update from a central installation directory (CID), there is also a central copy of INTERCHK.CFG in the CID. Whenever the InterCheck on-access scanner is installed or updated by a workstation from the CID, the central copy of INTERCHK.CFG is copied to the workstation, facilitating centralised configuration of INTERCHK.CFG.

- ❗ You must run the following command after carrying out any changes to this file in the CID

```
SETUP -UPDATE
```

to ensure the workstations detect the changed file.

The file is not case-sensitive.

It has four sections:

<b>[InterCheckGlobal]</b>	Recognised by all workstations
<b>[InterCheckWorkstation]</b>	Recognised by one or more named workstations
<b>[InterCheckOS2Global]</b>	Recognised by all OS/2 workstations
<b>[InterCheckOS2Workstation]</b>	Recognised by one or more named OS/2 workstations

The square brackets are part of the section names.

The two section names [...workstation] must be followed by a line

```
Address=xxx
```

Where xxx is the name of a workstation that will recognise the section. A section may include several address lines if more than one workstation is required to recognise the section.

- ❗ In OS/2 InterCheck the workstation name is specified by the line

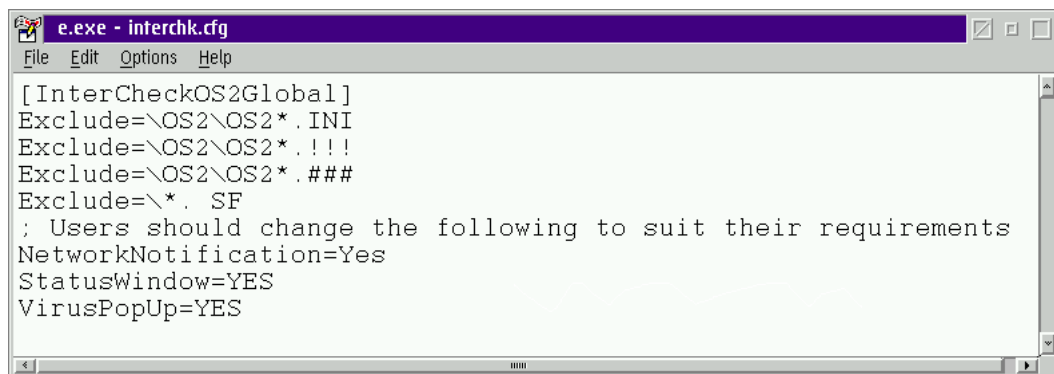
```
SET HOSTNAME=xxx
```

which must be included in the file CONFIG.SYS on each computer. Restart the computer for this change to take effect. You may find this line has already been inserted by the Sophos Anti-Virus installer.

The file contains some information by default, which is explained in section 8.2.

## 8.2 Configuration options for InterCheck for OS/2

The default InterCheck configuration file is as shown below.



```
e.exe - interchk.cfg
File Edit Options Help
[InterCheckOS2Global]
Exclude=\OS2\OS2*.INI
Exclude=\OS2\OS2*.*!!
Exclude=\OS2\OS2*.*###
Exclude=\*.SF
; Users should change the following to suit their requirements
NetworkNotification=Yes
StatusWindow=YES
VirusPopUp=YES
```

### **NetworkNotification=YES**

When InterCheck finds a virus, it will run the batch file NTFY.CMD in the CID, and send a virus notification to a named workstation.

This file may also be run if a virus is found during an immediate or scheduled scan.

### **StatusWindow=YES**

InterCheck Monitor runs constantly, recording the last file scanned by InterCheck.

### **VirusPopUp=YES**

When InterCheck finds a virus, a popup virus alert is displayed at the workstation.

To change any of these settings, change **YES** to **NO**.

You can add other commands to the file, as described below. If you have any non-OS/2 computers, you should also see the shared configuration options listed in [section 8.3](#).

### **AppendLogfile=YES | NO**

Normally when the OS/2 InterCheck scanner starts, it starts a new log file (the previous log is renamed with a .BAK extension, and previous .BAK logs are deleted). This may throw away valuable information about viruses found previously on this computer, so this option enables InterCheck to keep the existing log and append information to it each time the scanner starts. If this option is used, the log file can grow slowly until it fills the user's disk, unless the user prunes it from time to time. For this reason the default is not to append, but to start a new file each time the scanner starts.

### **CheckNetwork=YES | NO**

If set to YES (default), both files on file servers (network drives or UNC paths) and files on local drives will be scanned before access is allowed. If set to NO, only files on local drives will be scanned (set to NO only if it can be assumed that files on file servers have already been scanned at the server).

### **Exclude= <path>**

Excludes files from being scanned. Access is always allowed immediately, and there is no record of whether the file is infected. This option is used to exempt critical files which are known to contain non-infectable data or text, and which are intensively used. If this is not done, some applications (particularly legacy or poor quality ones) may run extremely slowly or even hang. The choice of files to be exempted is made by experiment if an application performs poorly.

Several Exclude entries may be given, one for each group of files to be excluded. A group is specified by use of wild cards \* and/or ? in the filename, in the normal OS/2 way. The following forms of entry are accepted:

d: Exclude all files on drive d:

a\*b.?c – Exclude files matching a\*b.?c in any directory on any drive.

d:a\*b.?c – Exclude files a\*b.?c in any directory on drive d:

\dir1\dir2\a\*b.?c – Exclude files a\*b.?c in directory \dir1\dir2 on any drive.

d:\dir1\dir2\a\*b.?c – Exclude files a\*b.?c in directory \dir1\dir2 on drive d:

A filename of '\*' is interpreted as '\*.\*' (any file).

A filename of '\*. ' means any file with a blank extension.

If a directory path is given it must be absolute (begin with a '\').

If a directory is given, a filename must be given as well.

It is not possible to specify a directory subtree in a single entry (OS/2 has no way to do this).

### **InfectedCacheLifetime=n**

The OS/2 InterCheck scanner remembers the names of infected files it has found, so as not to produce duplicate reports (OS/2 itself can make several attempts to access a single infected file). This memory is erased after the number of seconds specified with this lifetime qualifier, so that the user is reminded about the infected file when trying again to access it after a period of time. This is particularly important in the case of removable disks, which may be replaced in a drive inadvertently. The default memory lifetime is 5 seconds. The minimum lifetime is 1 second and the maximum is 2147483647 seconds (effectively disabling the reminder).

### **LogFile= <path>**

Specifies the drive, directory and name of the log file. The defaults for the drive and directory are those where the InterCheck programs are installed. The default for the filename is INTERCHK.LOG.

### **LogLevel=0..5**

Controls the amount of information written to the log file.

- 0 nothing except startup messages
- 1 fatal errors
- 2 virus alerts
- 3 nonfatal errors
- 4 warnings (default)
- 5 information messages (the maximum amount of information will be logged)

Each level also logs the information in all the levels above it.

### **ScanMode=FULL | QUICK**

Controls the scanning level used to scan for viruses. Full scans the complete contents of each file. Quick scans only those parts of each file that are most likely to contain viruses. The default is quick.

**StartUpReport=NONE | NORMAL | VERBOSE**

Controls the amount of configuration information logged when the InterCheck scanner starts. Default is VERBOSE.

NONE No information logged.

NORMAL Program banner and version, version of main virus data, number of viruses recognised.

VERBOSE The above, plus the virus engine version, plus a list of all virus identity files (IDEs) loaded.

**WorkThreads=n**

This sets the number of file access operations that can be processed simultaneously by the OS/2 InterCheck scanner. The default is 10, which should not normally be changed except under the advice of Sophos technical support. Using too small a value will probably cause the user's computer to hang, so that a restart would be required.

### 8.3 Configuration options shared with other versions of InterCheck

The [InterCheckGlobal] and [InterCheckWorkstation] sections are shared with versions of InterCheck that run on other operating systems. If you use only OS/2, you should use only OS/2-specific sections and the options described in [sections 8.1 and 8.2](#).

**CheckNetwork=YES | NO**

Same as above.

**Exclude=**

Same as above. Other versions of InterCheck may accept only simple exclusion specifications:

a?b.c – filename only; only '?' is recognised as a wild card.

d: – all files on drive d:

**PopUpDisplay=OFF**

Same as VirusPopUp= above. ERROR and VERBOSE both mean YES.

**StartUpDisplay=NONE | NORMAL | VERBOSE**

Same as StartUpReport= above.

**SweepVxDLogFile= <path>**

Same as LogFile= above.

**SweepVxDLogLevel=0..5**

Same as LogLevel= above.

**SweepVxDMode=FULL | QUICK**

Same as ScanMode= above.

## ***Troubleshooting***

## 9 Troubleshooting

This section provides answers to some common problems that you may encounter when using Sophos Anti-Virus for OS/2.

If your problem is not described in this section, refer to the Sophos website [www.sophos.com](http://www.sophos.com) which includes a support knowledgebase, virus analyses, the latest IDEs, product downloads and technical articles.

If your problem is not described on the website, contact Sophos [technical support](#).

### 9.1 Sophos Anti-Virus runs slowly

#### Full scan

By default, Sophos Anti-Virus performs a quick scan, which scans only the parts of each file that are likely to contain viruses. However, if scanning is set to full, it scans everything, and takes significantly longer to carry out a scan.

- ❗ **Full scanning is needed in order to detect some viruses, but should only be enabled on a case-by-case basis (e.g. on advice from Sophos technical support).**

#### Checking archive files

If checking of archive files is enabled, every archive will be unpacked to the depth specified. Scanning may therefore take much longer than if this option is not selected.

#### Checking all files or all sectors

If Sophos Anti-Virus has been configured to check all files and/or all sectors, it will take longer than if only checking executable files.

## 9.2 Virus fragment reported

If a virus fragment is reported, contact Sophos [technical support](#) for advice.

The report of a virus fragment indicates that part of a file matches part of a virus. There are three possible causes:

### **Variant of a known virus**

Many new viruses are based on existing ones, so that code fragments typical of a known virus may appear in files infected with a new one. If a virus fragment is reported, it is possible that Sophos Anti-Virus has detected a new virus, which could become active.

### **Corrupted virus**

Many viruses contain bugs in their replication routines that cause them to infect target files incorrectly. An inactive portion of the virus (possibly a substantial part) may appear within the host file, and this is detected by Sophos Anti-Virus. A corrupted virus cannot spread.

### **Database containing a virus**

When running a full scan, Sophos Anti-Virus may report that there is a virus fragment in a database file.



## ***Glossary and index***

## Glossary

<b>Boot sector virus</b>	A type of computer virus which subverts the initial stages of the boot process. A boot sector virus attacks either the master boot sector or the DOS boot sector.
<b>Boot sector</b>	The part of the operating system which is first read into memory when a PC is switched on (booted). The program stored in the boot sector is then executed, which loads the rest of the operating system from the system files on disk.
<b>CMD</b>	The extension given to 'command' filenames in OS/2. A command file may be written in the OS/2 scripting language REXX, or may simply contain a series of OS/2 commands. STARTUP.CMD is a special command file which is executed whenever OS/2 is started, and can be used to configure OS/2 to a user's requirements.
<b>Hexadecimal</b>	A system of counting using number base 16. The numbers 10 to 15 are represented by the characters 'A' through 'F' respectively. Hexadecimal is often abbreviated to Hex. Each Hex digit is equivalent to four bits (half a byte) of information.
<b>IDE</b>	Virus identity file; enables Sophos Anti-Virus to detect a specific virus. You need IDEs to protect your computer against viruses discovered since your version of Sophos Anti-Virus was compiled.
<b>InterCheck/InterCheck Client</b>	A component of Sophos Anti-Virus that intercepts files as they are accessed, and grants access only to those that are virus free.
<b>LAN</b>	Local Area Network; a data communications network covering a limited area (up to several kilometres in radius) with moderate to high data transmission speeds.

<b>Macro virus</b>	A type of virus that uses macros in a data file to become active in memory and attach itself to other data files. Unlike other types of virus, macro viruses can attain a degree of platform independence.
<b>Master boot sector</b>	The first physical sector on the hard disk (sector 1, head 0, track 0) which is loaded and executed when the PC is booted. It contains the partition table as well as the code to load and execute the boot sector of the 'active' partition. Common point of attack by boot sector viruses.
<b>Polymorphic virus</b>	Self-modifying encrypting virus.
<b>SWEEP</b>	The component of Sophos Anti-Virus that provides immediate and scheduled virus scanning and disinfection.
<b>UNC</b>	Universal Naming Convention; a standard system for naming network drives, e.g. the UNC directory \\MAIN\USERS\ would refer to the USERS directory on the server called MAIN.
<b>Virus pattern</b>	A sequence of bytes extracted from a virus and used for virus recognition.

# Index

## A

- absolute sector 47
  - scanning 49
- archive files
  - scanning 16, 32, 74
  - scanning via the CLI 54, 63

## B

- boot image, CD 55
- boot manager
  - and disinfection 24
- boot sector
  - disinfection 20, 33

## C

- CD boot image 55
- checking all files 10, 74
  - via the CLI 54
- compressed files
  - scanning via the CLI 63

## D

- Diet 63
- disinfection 19–25, 56
  - automatic 33–34
  - on systems with boot manager 24
- disk sectors
  - checking via the CLI 47
- documents
  - disinfection 20, 24, 33

## E

- email scanning 32
- excluding files from scanning 14, 40
- executables
  - files treated as 40
  - limiting scanning to 10

## F

- file server
  - checking via the CLI 14, 57
- floppy disk
  - checking via the CLI 14
  - disinfecting boot sectors 22
- full scan 13, 31, 50, 74
  - via the CLI 57

## H

- hard disk
  - checking via the CLI 13
  - disinfecting boot sectors 21

## I

- IDE files
  - specifying location 57
- immediate scanning 9–25
  - adding items for scan 10–25
  - removing items from scan 10
  - starting 9
- infected files
  - dealing with 20
- integrity check 55
- InterCheck
  - configuring 67–72
- InterCheck Monitor 17

## L

- log file 39
- logical sector 47
  - scanning 48
- LZEXE 63

## M

- macro virus
  - disinfection 33
  - removal 24
- mailbox scanning 32
- master boot sector
  - replacing 22
- MIME files 58, 59

## N

- NTFY.CMD 68

## O

- on-access scanning
  - configuring 67
- on-demand scanning 13–25
  - configuring 28–38
  - configuring via the CLI 44–66
- on-screen log
  - clearing 41
- Outlook Express mailboxes 59, 61

## P

- pattern (of virus)
  - adding 51
- physical sector 47
  - scanning 49
- PKLite 63
- positive overwriting
  - of infected files 63
- programs
  - dealing with infected 23
  - disinfection 33
- progress bar
  - displaying 42

## Q

- quick scan 13, 31, 50

## R

- recursive scanning
  - via the CLI 62
- report file 37
- rights on NetWare 14

## S

- scanning CD boot image 55
- scheduled scanning
  - adding a job 11
  - configuring via the CLI 15, 44–66
  - configuring via the GUI 28–38
  - copying jobs 38
  - editing a job 12
  - job list 11
  - removing a job 12
- security report 61
- SETUP -UPDATE 67
- shredding
  - of infected files 63
- silent running
  - CLI version 63
- STARTUP.CMD 55
- subfolders
  - scanning 10
- SWEEP.ARE 14, 45
- SWEEP.PAT 51

## V

- virus
  - analyses 41
  - boot sector 33
  - disinfection 19–25, 33–34, 52, 56
  - Form 24
  - fragment 75
  - macro 24
  - pattern
    - adding 51
  - recovery from 25
  - removal 52, 59, 62, 63
  - warning 35–72
  - Winword/ShareFun 24

## Z

- zip bombs 60

## Technical support

For technical support, visit [www.sophos.com/support](http://www.sophos.com/support).

If you contact technical support, provide as much information as possible, including the following:

- Sophos software version number(s)
- operating system(s) and patch level(s)
- the exact text of any error messages.

Copyright 2003–2007 Sophos Group. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the licence terms or you otherwise have the prior permission in writing of the copyright owner.

Sophos and Sophos Anti-Virus are registered trademarks of Sophos Plc and Sophos Group. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.